

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

FARHAD AZIMA,)	
)	
Plaintiff,)	
)	
v.)	1:20CV954
)	
NICHOLAS DEL ROSSO and VITAL)	
MANAGEMENT SERVICES, INC.,)	
)	
Defendants.)	

**ORDER AND RECOMMENDATION
OF UNITED STATES MAGISTRATE JUDGE**

This matter comes before the undersigned magistrate judge for a recommended ruling on a motion to dismiss by Defendants Nicholas Del Rosso and Vital Management Services, Inc. (collectively “Defendants”) pursuant to Federal Rule of Civil Procedure 12(b)(6). (Docket Entry 31.) Also pending before the Court are three motions by Plaintiff Farhad Azima: 1) a motion for leave to file supplemental materials in support of his response to Defendants’ motion to dismiss (Docket Entry 45); 2) a motion to schedule an initial pretrial conference and to initiate Rule 26(f) and Local Rule 16.1(f) conferences, or in the alternative, for an order commencing discovery pending a pretrial conference to be set on a later date (Docket Entry 36); and 3) a renewed motion to schedule an initial pretrial conference or commence discovery (Docket Entry 52). For the following reasons, the undersigned will recommend denying Defendants’ motion to dismiss as to Counts III, VIII, X, and XI of Plaintiff’s complaint but will recommend granting Defendants’ motion as to Plaintiff’s other seven claims. Additionally, the undersigned will deny Plaintiff’s motion to supplement his

response to Defendants' motion to dismiss and grant in part Plaintiff's motions to schedule an initial pretrial conference and commence discovery.

I. BACKGROUND

Plaintiff initiated this action against Defendants on October 15, 2020. (*See* Compl., Docket Entry 1.) Plaintiff, a U.S. citizen who resides in Kansas City, Missouri, alleges that Defendants "oversaw and directed the hacking of Plaintiff" and "stole [his] computer data, including emails and trade secrets." (Compl. ¶¶ 1, 10.) Defendant Del Rosso is the president, owner, and sole employee of Defendant Vital Management Services, Inc. ("Vital"), a company based in Chapel Hill, North Carolina that provides investigative services. (*Id.* ¶¶ 11-12.)

To summarize the allegations in the complaint, Plaintiff alleges that in early 2015 the Ras Al Khaimah Investment Authority ("RAKIA"), the state investment entity for the government of Ras Al Khaimah with whom Plaintiff was engaged in a business dispute, began to discuss a plan with its associates to "target" Plaintiff. (*Id.* ¶¶ 2, 7, 14.) To that end, Plaintiff alleges that Defendants were hired by Dechert LLP through partner Neil Gerrard to hack Plaintiff on behalf of RAKIA. (*Id.* ¶¶ 2, 7.) Plaintiff alleges that Defendants in turn hired an Indian company called CyberRoot Risk Advisory Private Limited ("CyberRoot") and paid CyberRoot more than one million dollars to orchestrate the sending of phishing and spear-phishing emails to Plaintiff, which "successfully induced [him] to unwittingly provide . . . passwords for his accounts." (*Id.* ¶¶ 2, 5, 6.) Plaintiff alleges that another India-based hacking company called BellTroX InfoTech Services ("BellTroX") assisted CyberRoot in hacking Plaintiff. (*Id.* ¶ 3.) As a result, data from Plaintiff's computers and emails

accounts was disclosed on internet blog sites on or about August 7, 2016. (*Id.* ¶¶ 6, 20.) In May and June 2018 and again in June 2019 the blog sites were modified to include new links to publicly available sites containing Plaintiff's stolen data." (*Id.* ¶¶ 24-26, 53.)

Plaintiff alleges that RAKIA's goal in hiring Defendants to coordinate the hacking of Plaintiff was to "weaponize that data in an attempt to ruin [Plaintiff]" and to use the stolen data as evidence in a lawsuit against Plaintiff in England. (*Id.* ¶¶ 2, 7.) Plaintiff alleges that during the English lawsuit, which was initiated by RAKIA in September 2016, Defendant Del Rosso and others "created a false evidentiary trail to cover up their and RAKIA's responsibility for the hacking" and to suggest that the hacked material had been innocently found. (*Id.* ¶¶ 7, 22, 33.) Plaintiff raised the hacking as a defense in that lawsuit, in addition to using it as the basis of a counterclaim against RAKIA. (*Id.*) Plaintiff asserts that the English court ruled that RAKIA and others "had lied about how they obtained [Plaintiff's] stolen data. (*Id.* ¶ 8.) In particular, Plaintiff alleges that Defendant Del Rosso gave false testimony denying knowledge of how the stolen emails were obtained. (*Id.*) Plaintiff alleges that as a result of Defendants' actions, Plaintiff has suffered "significant financial and reputational damage." (*Id.* ¶ 9.)

Based on these allegations, Plaintiff raises federal law claims for violations of the Electronic Communications Privacy Act ("Wiretap Act") (Count I), conspiracy to disclose communications obtained in violation of the Wiretap Act (Count II), and misappropriation of trade secrets (Count III) against all Defendants, in addition to North Carolina state law claims for computer trespass (Count IV), conversion (Count V), identity theft (Count VI), publication of personal information (Count VII), violation of the Trade Secrets Protection

Act (VIII), violation of the Unfair and Deceptive Trade Practices Act (IX), civil conspiracy (Count X), and invasion of privacy (Count XI). (*Id.* ¶¶ 44-139.)

Defendants filed the foregoing motion to dismiss on December 21, 2020. (Docket Entries 31.) Plaintiff filed a response in opposition, and Defendants filed a reply. (Docket Entries 34, 39.) Several weeks later, Plaintiff filed a motion to supplement his response in opposition to Defendants' motion to dismiss. (Docket Entry 45.) Defendants oppose Plaintiff's motion. (Docket Entry 47.) Plaintiff also filed a motion requesting that the Court schedule an initial pretrial conference in this matter, or in the alternative issue an order commencing discovery pending the scheduling of an initial pretrial conference. (Docket Entry 36.) Defendants also oppose this motion. (Docket Entry 43.) All four motions are ripe for disposition. The undersigned will address each in turn.

II. DISCUSSION

A. Defendants' Motion to Dismiss

Defendants move to dismiss Plaintiff's complaint pursuant to Federal Rule of Civil Procedure 12(b)(6). (*See* Docket Entry 31.) A motion to dismiss pursuant to Rule 12(b)(6) tests the sufficiency of the complaint. *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (1999). A complaint that does not "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face'" must be dismissed. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct." *Id.*; *see also Simmons v. United Mortg. & Loan Inv., LLC*, 634 F.3d 754, 768 (4th Cir. 2011) ("On a Rule 12(b)(6)

motion, a complaint must be dismissed if it does not allege enough facts to state a claim to relief that is plausible on its face.”) (citations and quotations omitted). The “court accepts all well-pled facts as true and construes these facts in the light most favorable to the plaintiff,” but does not consider “legal conclusions, elements of a cause of action, and bare assertions devoid of factual enhancement[.] . . . unwarranted inferences, unreasonable conclusions, or arguments.” *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 255 (4th Cir. 2009) (citations omitted). In other words, the standard requires a plaintiff to articulate facts, that, when accepted as true, demonstrate the plaintiff has stated a claim that makes it plausible he is entitled to relief. *Francis v. Giacomelli*, 588 F.3d 186, 193 (4th Cir. 2009) (quoting *Iqbal*, 556 U.S. at 678, and *Twombly*, 550 U.S. at 557).

A motion to dismiss pursuant to Rule 12(b)(6) must be read in conjunction with Federal Rule of Civil Procedure 8(a)(2). Rule 8(a)(2) requires only “a short and plain statement of the claim showing that the pleader is entitled to relief,” so as to “give the defendant fair notice of what the . . . claim is and the grounds upon which it rests” *Twombly*, 550 U.S. at 555 (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). Rule 8 does not, however, unlock the doors of discovery for a plaintiff armed with nothing more than conclusions. Fair notice is provided by setting forth enough facts for the complaint to be “plausible on its face” and “raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true (even if doubtful in fact)” *Id.* at 555 (internal citations omitted). “Rule 12(b)(6) does not countenance . . . dismissals based on a judge’s disbelief of a complaint’s factual allegations.” *Id.* at 556 (quoting *Scheuer v. Rhodes*, 416, U.S. 232, 236 (1974)).

In their initial brief in support of their motion to dismiss, Defendants argued that dismissal of Plaintiff's complaint in its entirety is warranted for three reasons: 1) Plaintiff's claims are time-barred; 2) Plaintiff's action is barred by claim and issue preclusion; and 3) Plaintiff's complaint fails to state claims for relief under both federal and North Carolina law. (*See generally* Docket Entry 32.) However, Plaintiff notified the Court in his motion to supplement his response in opposition to Defendant's motion to dismiss that the judgment against him in the High Court of Justice Business and Property Courts of England and Wales is now on appeal. (Docket Entry 49.) In light of this new development, Defendants have withdrawn their preclusion argument "without prejudice to its later assertion." (*See* Docket Entry 50 at 1.)¹ Thus, the undersigned addresses below whether Plaintiff's claims as alleged are time-barred, and if not, whether they plausibly entitle him to relief, but will not address whether Plaintiff's claims are precluded.

1. Are Plaintiff's claims time-barred?

Defendants first argue that Plaintiff's eleven claims are time-barred by the applicable statute of limitations. (Docket Entry 32 at 7-8.) (*Id.*) A statute of limitations defense "can be the basis of a motion to dismiss under Rule 12(b)(6)." *Dickinson v. Univ. of N.C.*, 91 F. Supp. 3d 755, 763 (M.D.N.C. 2015) (citing *Dean v. Pilgrim's Pride Corp.*, 395 F.3d 471, 474 (4th Cir. 2005)). However, for a statute-of-limitations defense to succeed at the motion to dismiss stage, "all facts necessary to show the time bar must clearly appear 'on the face of the complaint.'" *Id.* (citing *Goodman v. Praxair, Inc.*, 494 F.3d 458, 464 (4th Cir. 2007); *see also Morrison v. George E.B. Holding*, No. 7:11-CV-168-BO, 2012 WL 1132787, at *3 (E.D.N.C.

¹ Page numbers in this recommendation refer to the page numbers found at the bottom right-hand corner of the litigation documents as they appear in this Court's CM/ECF system.

Apr. 4, 2012) (“Generally, an affirmative defense that a complaint is barred by a statute of limitations may not form the basis of Rule 12(b)(6) dismissal unless all of the facts necessary for the defense appear on the face of the complaint.”).

The parties do not dispute the statute of limitations periods that apply to each of Plaintiff's eleven claims. (*See* Docket Entry 34 at 3 n. 1; Docket Entry 32 at 7-8.) Plaintiff's claim brought pursuant to the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1, has a four-year statute of limitations. *See* N.C. Gen. Stat. § 75-16.2. Plaintiff's federal misappropriation of trade secrets claim brought pursuant to 18 U.S.C. §§ 1831, 1832, 1836 has a three-year limitations period. *See* 18 U.S.C. § 1836(d). The majority of Plaintiff's North Carolina state law claims also have a three-year limitations period. *See* N.C. Gen. Stat. § 1-52(4) (conversion); N.C. Gen. Stat. § 1-539.2C(c) (identity theft and publication of personal information); N.C. Gen. Stat. § 66-157 (Trade Secrets Protection Act); N.C. Gen. Stat. § 1-52(5) (invasion of privacy); *BDM Investments v. Lenhil, Inc.*, 826 S.E.2d 746, 764 (N.C. Ct. App. 2019) (civil conspiracy). A two-year limitations period applies to Plaintiff's claims brought pursuant to the Wiretap Act. *See* 18 U.S.C. §§ 2511(1)(c), 2520(e). Finally, Plaintiff's computer trespass claim is subject to a one-year statute of limitations. *See* N.C. Gen. Stat. § 14-458; N.C. Gen. Stat. § 1-54.

However, Defendants argue in their brief that the statute of limitations for each of Plaintiff's actions had accrued by September 2016 at the latest, when Plaintiff became aware that he had been hacked and initiated a separate lawsuit against RAKIA in the United States District Court for the District of Columbia. (Docket Entry 32 at 8.) Thus, because all of Plaintiff's claims are subject to a statute of limitations of four years or less and he did not file

the instant lawsuit until October 2020, Defendants argue that none of Plaintiff's claims were timely filed and they should all be dismissed on that basis. (*Id.* at 7-9.) In response, Plaintiff argues that his claims are not time-barred because: 1) Defendants fraudulently concealed their misconduct, thus tolling the statute of limitations; and 2) Defendants engaged in actionable conduct more recently than 2016. (Docket Entry 34 at 4, 6.)

Upon a careful review of the complaint and the parties' arguments, the undersigned only recommends dismissing two of Plaintiff's claims as time-barred at this early stage in the litigation. Plaintiff's eleven claims are subject to various distinct accrual rules. For example, Plaintiff's federal Wiretap Act claims (Counts I and II) accrued when plaintiff "first [had] a reasonable opportunity to discover the violation." 18 U.S.C. § 2520(e). Likewise, Plaintiff's federal misappropriation of trade secrets action (Count III) accrued on the date that "the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered." 18 U.S.C. § 1836(d). Plaintiff's state Trade Secret Protection Act (Count VIII), civil conspiracy (Count X), and invasion of privacy (Count XI) claims follow similar accrual rules based on the discovery of the violation.²

Though Defendants assert that Plaintiff became aware of the hacking in September 2016 at the latest when he filed a lawsuit related to the hacking in the District of Columbia,

² Plaintiff's misappropriation of trade secrets claim accrued when "the misappropriation complained of [was] or reasonably should have been discovered." N.C. Gen. Stat. § 66-157. Plaintiff's common law civil conspiracy and common law invasion of privacy claims appear to have accrued when "physical damage to his property becomes apparent or ought reasonably to have become apparent to the claimant, whichever event first occurs." *Alexander v. City of Greensboro*, No. 1:09-CV-293, 2011 WL 3360644, at *13 n. 21 (M.D.N.C. Aug. 3, 2011) (citing N.C. Gen. Stat. § 1-52(16)).

the complaint itself does not include allegations specifying when Plaintiff discovered the hacking or Defendants' involvement, nor does it mention the lawsuit he filed in the District of Columbia. Thus, the undersigned is unable to determine from the face of Plaintiff's complaint precisely when such claims accrued and therefore does not recommend dismissing Counts I, II, III, VIII, X, and XII on statute of limitations grounds. *See Waugh v. Elan Fin. Serv.*, No. CV 3:17-4378, 2018 WL 2976430, at *5 (S.D.W. Va. June 13, 2018) (“[T]he Court therefore cannot determine from the face of the Complaint the date of accrual of Plaintiffs’ causes of action. Where it is not clear from the face of the Complaint whether the statute of limitations has run, dismissal is inappropriate.”) (citing *Goodman*, 494 F.3d at 466).

In addition, as Plaintiff points out (*see* Docket Entry 34 at 6), his identity theft and publication of personal information claims (Counts VI and VII) accrued on the date that he discovered, or reasonably should have discovered, *the identity of the wrongdoers*. *See* N.C. Gen. Stat. § 1-539.2C(c). Plaintiff's complaint alleges that he did not become aware of Defendants' involvement in the hacking until “recently.” (Compl. ¶ 36; *see also id.* ¶ 127 (“Plaintiff discovered that Defendants committed unfair and deceptive acts or practices that injured him on or about August 28, 2020 following an investigation.”).) Accepting this statement as true, the statute of limitations had not run when Plaintiff filed this lawsuit just two months later in October 2020. Alternatively, whether Plaintiff “reasonably should have discovered” Defendants' identity earlier cannot be determined from the face of the complaint. Plaintiff does not describe his efforts to discover Defendants' identity or involvement prior to August 2020, and it is not apparent that the type of investigation that revealed Defendants' involvement on or about August 28, 2020 could have been conducted

beforehand. Therefore, the undersigned finds that dismissing these two claims (Counts VI and VII) on statute of limitations grounds is also inappropriate.

Plaintiff's unfair and deceptive trade practices claim (Count IX) accrued "when the violation occur[red]." *Hetzl v. JPMorgan Chase Bank, N.A.*, No. 4:13-CV-236-BO, 2014 WL 7336863, at *3 (E.D.N.C. Dec. 22, 2014) (citing *Hinson v. United Fin. Servs., Inc.*, 473 S.E.2d 382, 387 (N.C. Ct. App. 1996)). Plaintiff alleges that "Defendants published Azima's private information on blog sites hosting WeTransfer links in May and June of 2018, and again in June of 2019" and alleges that the publication of his confidential information constitutes a violation of N.C. Gen. Stat. § 75-1.1. (Compl. ¶¶ 93, 122.) Given that the statute of limitations for an unfair and deceptive trade practices claim is four years, *see* N.C. Gen. Stat. § 75-16.2, and Plaintiff has alleged a violation of this statute as recently as 2019, dismissal of Count IX of Plaintiff's complaint as time barred is not warranted.

The only claims that may appropriately be dismissed as time barred at this stage in the litigation are Plaintiff's state law computer trespass (Count IV) and conversion (Count V) claims. As alleged in Plaintiff's complaint, Defendants committed computer trespass by using Plaintiff's "computer and computer network with the intent to make or cause to be made unauthorized copies of Plaintiff's computer data." (Compl. ¶¶ 75-79.)³ In support of this claim, Plaintiff alleges that Defendants instructed CyberRoot to hack Plaintiff's computer and computer network. (*Id.* ¶ 79.) CyberRoot gained access to Plaintiff's email

³ *See* N.C. Gen. Stat. § 14-458(5) ("[I]t shall be unlawful for any person to use a computer or computer network without authority and with the intent to . . . [m]ake or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.").

accounts and computers and used that access to make copies of Plaintiff's "trade secrets, confidential business information, and personal information and communications that would provide Defendants and their co-conspirators leverage over Plaintiff." (*Id.* ¶ 78; *see also id.* ¶¶ 14-18.) The hacking occurred on or before August 7, 2016. (*See id.* ¶¶ 20-21.)

The undersigned has been unable to locate a specific accrual rule for computer trespass claims but notes that "[a] cause of action generally accrues and the statute of limitations begins to run as soon as the right to institute and maintain a suit arises." *Hunter v. Guardian Life Ins. Co. of Am.*, 593 S.E.2d 595, 601 (N.C. Ct. App. 2004) (quoting *Penley v. Penley*, 332 S.E.2d 51, 62 (N.C. 1985)). The statute of limitations for a computer trespass claim is only one year. *See* N.C. Gen. Stat. § 1-539.2A and § 1-54. While it is not clear from the face of the complaint exactly when Plaintiff became aware that he had been hacked, it is clear from the face of the complaint that Plaintiff had this knowledge more than one year before the instant lawsuit was filed. The complaint states that RAKIA initiated a lawsuit against Plaintiff in September 2016 and Plaintiff used the hacking as a defense and as the basis for a counterclaim. (*See* Compl. ¶¶ 7, 33.) The complaint mentions that the English case went to trial in January 2020. (*Id.* ¶ 34.) These dates indicate that Plaintiff's counterclaim, which would have required him to have knowledge of the hacking, was filed more than a year before the instant lawsuit.

Furthermore, the complaint does not contain any allegation that Plaintiff's computers or accounts were hacked again following the original hacking that occurred on or before August 7, 2016. While Plaintiff has alleged that Defendants took actions to publish or disseminate Plaintiff's stolen data in 2018 and 2019 (*see* Compl. ¶ 93), Plaintiff has not

indicated that Defendants accessed Plaintiff's computer or computer networks with the intent to make new unauthorized copies on those dates or any more recently so as to restart the statute of limitations. Therefore, it is clear from the face of the complaint that Plaintiff had "the right to institute and maintain a suit" for computer trespass more than one year prior to the filing of this lawsuit on October 15, 2020. Accordingly, the undersigned recommends dismissing Plaintiff's computer trespass claim (Count IV) as time barred.

Regarding plaintiff's conversion claim, Plaintiff correctly states in his complaint that "[u]nder North Carolina law, conversion occurs when a defendant wrongfully possesses or converts property under the ownership of the Plaintiff." (Compl. ¶ 83.) *See also Intercollegiate Women's Lacrosse Coaches Ass'n v. Corrigan Sports Enterprises, Inc.*, 505 F. Supp. 3d 570, 585–86 (M.D.N.C. 2020) ("The two essential elements of [a conversion] claim are (1) ownership in the plaintiff and (2) wrongful possession or conversion by the defendant." (citing *Variety Wholesalers, Inc. v. Salem Logistics Traffic Servs., LLC*, 723 S.E.2d 744, 747 (N.C. 2012))). Plaintiff alleges that Defendants "conspired to wrongfully obtain and exercise possession of Plaintiff's computer data, documents, spreadsheets, communications, and other files." (Compl. ¶ 84.) Defendants instructed CyberRoot to hack Plaintiff, and upon the successful hack, "converted Plaintiff's computer data." (*Id.* ¶ 85.)

"As a general rule, [a conversion] claim accrues, and the statute of limitations begins to run, when the unauthorized assumption and exercise of ownership occurs—not when the plaintiff discovers the conversion." *Ferro v. Vol Vo Penta of the Americas, LLC*, No. 5:17-CV-194-BO, 2017 WL 3710071, at *4 (E.D.N.C. Aug. 28, 2017), *aff'd sub nom. Ferro v. Volvo Penta of the Americas, LLC*, 731 F. App'x 208 (4th Cir. 2018) (quoting *Celgard, LLC v. LG Chem*,

Ltd., No. 3:14-CV-00043-MOC-DC, 2015 WL 2412467, at *16 (W.D.N.C. May 21, 2015)); *see also First Invs. Corp. v. Citizens Bank, Inc.*, 757 F. Supp. 687, 690 (W.D.N.C. 1991), *aff'd*, 956 F.2d 263 (4th Cir. 1992) (“The general rule thus appears to be that conversion actions accrue upon the conversion itself rather than upon its discovery.”). Thus, Plaintiff’s conversion claim accrued at the time that Defendants converted his computer data, which according to the complaint, occurred on or before August 7, 2016. (Compl. ¶¶ 20-21.) Since the statute of limitations for conversion claims is three years, *see* N.C. Gen. Stat. § 1–52(4), and Plaintiff’s complaint does not allege that Defendants took possession of any additional data or documents of Plaintiff’s during the three years preceding the filing of this lawsuit, the undersigned recommends that Plaintiff’s conversion claim (Count V) be dismissed on statute of limitations grounds.

The undersigned does not find that fraudulent concealment by Defendants precludes the operation of the statutes of limitations as to these two claims. As both parties suggest in their briefs (*see* Docket Entry 34 at 5; Docket Entry 39 at 2 n. 2), and consistent with this Court’s reasoning in *Jones v. BMW of N. Am., LLC*, because these two claims are subject to North Carolina statutes of limitations, “North Carolina tolling laws may be the more appropriate law for decision” for these state law claims. No. 1:20-CV-00057, 2020 WL 5752808, at *4 n. 4 (M.D.N.C. Sept. 25, 2020) (citing *Hemenway v. Peabody Coal Co.*, 159 F.3d 255, 265 (7th Cir. 1998) (“When state law supplies the period of limitations, it also supplies the tolling rules.”)). According to North Carolina law, the doctrine of equitable estoppel may “preclude a defendant’s pleading of the statute of limitations” where a plaintiff can establish the following elements as related to the party estopped:

(1) Conduct which amounts to a false representation or concealment of material facts, or, at least, which is reasonably calculated to convey the impression that the facts are otherwise than, and inconsistent with, those which the party afterwards attempts to assert; (2) intention or expectation that such conduct shall be acted upon by the other party, or conduct which at least is calculated to induce a reasonably prudent person to believe such conduct was intended or expected to be relied and acted upon; (3) knowledge, actual or constructive, of the real facts.

Wilkerson v. Christian, No. 1:06CV00871, 2008 WL 483445, at *7, 11 (M.D.N.C. Feb. 19, 2008) (quoting *Hawkins v. M. & J. Fin. Corp.*, 77 S.E.2d 669, 672 (N.C. 1953)). In addition, as related to the party claiming the estoppel, a plaintiff must show:

(1) lack of knowledge and the means of knowledge of the truth as to the facts in question; (2) reliance upon the conduct of the party sought to be estopped; and (3) action based thereon of such a character as to change his position prejudicially.

Id. For equitable estoppel to apply, “a plaintiff must plead supporting facts with particularity and demonstrate that defendant’s representations delayed her from filing suit.” *Worrell v. A Woman’s View, P.A.*, No. 518CV00178MOCDSC, 2019 WL 427336, at *3 (W.D.N.C. Feb. 4, 2019) (citing *Duke Univ. v. St. Paul Mercury Ins. Co.*, 384 S.E.2d 36, 42 (N.C. Ct. App. 1989)).⁴

⁴ To some extent, North Carolina courts have also recognized fraudulent concealment as a separate basis for tolling the statute of limitations. *Wilkerson*, 2008 WL 483445, at *11 (“The Supreme Court of North Carolina has, by implication, approved of the doctrine of fraudulent concealment as a tolling doctrine.”) (collecting cases). However, in both *Jones* and *Wilkerson*, this Court has noted that there is some confusion among North Carolina courts as to the effect of fraudulent concealment on a statute of limitations and the elements that must be shown to invoke it. *See Jones*, 2020 WL 5752808, at *4 n. 4 (“North Carolina courts do not typically recognize fraudulent concealment as a mechanism for tolling the statute of limitations”); *Wilkerson*, 2008 WL 483445, at *11 n. 13 (“The parties did not cite, nor was the court able to identify, a North Carolina decision that fully sets forth the elements of fraudulent concealment as a tolling doctrine [as opposed to a cause of action for actual fraud].”). The undersigned has not identified a more recent North Carolina decision that clarifies these issues. Moreover, the parties appear to agree that the proper standard for

Here, the undersigned does not find that Plaintiff has alleged sufficient facts in his complaint to establish the element of reliance that is necessary to invoke the North Carolina doctrine of equitable estoppel to preclude the application of the statute of limitations to his computer trespass and conversion claims. As previously mentioned, Plaintiff accuses Defendant Del Rosso of attempting “to lay a false ‘paper trail’ of discovery” by exchanging emails with Gerrard in August 2016 and falsely denying his involvement in the hacking during the English proceedings. (Compl. ¶¶ 35-36.) However, Plaintiff has not alleged how or why this “false paper trail” prevented him from filing suit against Defendants within the limitations period. The complaint contains no indication that the “false” emails exchanged by Gerrard and Defendant Del Rosso effectively deceived Plaintiff into believing that some entity other than RAKIA and its agents was responsible for the hacking.

Furthermore, to the extent that Plaintiff grounds his fraudulent concealment arguments in the false witness statement and testimony given by Defendant Del Rosso in conjunction with the English proceedings, these statements do not appear to have been made until the year 2020 (*see* Compl. ¶¶ 8, 34), at which point the one-year statute of limitations for Plaintiff’s computer trespass claim and the three-year limitations period for

analyzing Plaintiff’s state law claims, regardless of how they have named it, is the equitable estoppel standard recited herein. (*See* Docket Entry 34 at 5; Docket Entry 39 at 2 n. 2 (citing *Ferro v. Vol Vo Penta of the Americas, LLC*, No. 5:17-CV-194-BO, 2017 WL 3710071, at *4 (E.D.N.C. Aug. 28, 2017), *aff’d sub nom. Ferro v. Volvo Penta of the Americas, LLC*, 731 F. App’x 208 (4th Cir. 2018) (reciting equitable estoppel elements).) Finally, to the extent that fraudulent concealment has been recognized by North Carolina courts as a tolling doctrine, a plaintiff must still “allege reliance on the defendant’s misrepresentations or omissions.” *Wilkerson*, 2008 WL 483445 at *12. Because the undersigned has determined that Plaintiff has not sufficiently alleged reliance, application of the doctrine of fraudulent concealment would not alter the result reached herein.

Plaintiff's conversion claim would have already run. Thus, Plaintiff cannot plausibly argue that his reliance on such statements prevented him from filing his computer trespass and conversion claims in a timely manner. In sum, Plaintiff has made no specific allegations explaining how he relied upon Defendant's false statements to his detriment. Without such allegations, Plaintiff cannot meet his burden of proving the essential elements of equitable estoppel. *See Bankaitis v. Allstate Ins. Co.*, 229 F. Supp. 3d 381, 387 (M.D.N.C. 2017) ("It is the party asserting equitable estoppel who bears the burden of proving the essential elements.") (citing *State Farm Mut. Auto. Ins. Co. v. Atl. Indem. Co.*, 468 S.E.2d 570, 575 (N.C. Ct. App. 1996)). The undersigned finds that the doctrines of equitable estoppel and fraudulent concealment do not preclude the normal operation of the statutes of limitations that apply to Plaintiff's computer trespass and conversion claims.⁵ Therefore, the undersigned recommends dismissing Plaintiff's computer trespass (Count IV) and conversion (Count V) claims as time barred. As to the other nine claims, the undersigned will discuss below whether they state a plausible claim for relief as alleged.

⁵ Plaintiff's second argument in response to Defendants' contention that all his claims are time-barred is that Defendants engaged in actionable conduct within the relevant limitation periods. (*See* Docket Entry 34 at 6-8.) The paragraphs in the complaint that Plaintiff argues describe "actionable conduct" that allegedly occurred in 2018 and 2019 state that "[i]n May and June 2018, the blog sites [where Plaintiff's data had originally been posted] were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data" and that again, "[i]n June 2019, the links on the blog sites were modified to include new WeTransfer links containing some of Azima's stolen data. (Compl. ¶¶ 24, 26.) These actions in 2018 and 2019 involve the publication and disclosure of the originally stolen data. (*Id.* ¶¶ 23, 53, 93, 98.) Because, as explained above, Plaintiff's computer trespass and conversion claims are tied to the actual hacking in 2016 (and not the subsequent dissemination of the data), Plaintiff's argument is unavailing as to these two counts.

2. Do Plaintiff's surviving claims state plausible claims for relief?

a. Wiretap Act (Count I)

Plaintiff brings his first claim pursuant to the federal Electronic Communications Privacy Act ("Wiretap Act"). (Compl. ¶¶ 44-53.) The subsection of the law referenced in Count I of Plaintiff's complaint prohibits a person from

intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

18 U.S.C. § 2511(1)(c). "Furthermore, section 2520 allows the victim of the interception to bring a civil action against the section 2511 violator." *DirecTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 447 (M.D.N.C. 2004); *see also* 18 U.S.C. § 2520. Plaintiff alleges that Defendants

directed CyberRoot to intentionally disclose large quantities of Azima's intercepted data by instructing that the data be posted on BitTorrent and WeTransfer. Links to those BitTorrent and WeTransfer sites were added to the blog sites that CyberRoot created. CyberRoot worked with BellTroX and at the direction of the Defendants to conduct the hacking and post the intercepted data.

(Compl. ¶ 49.) Plaintiff further alleges that Defendants knew or had reason to know that the information was obtained through interception. (*Id.* ¶ 52.)

Defendants argue that Plaintiff fails to state a claim "because there is no civil liability for secondary or conspiracy conduct" under the Wiretap Act. (Docket Entry 32 at 17.) Defendants point out that Plaintiff "does not allege that Defendants *themselves* intercepted, disclosed, or used Azima's data [but rather] that CyberRoot and/or BellTroX did so." (*Id.*

(emphasis in original) (citing Compl. ¶¶ 16-19.) Indeed, regarding civil damages the Wiretap Act provides that in general, “any person whose wire, oral or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from *the person or entity*, other than the United States, *which engaged in that violation such relief as may be appropriate.*” 18 U.S.C. § 2520(a) (emphasis added). The Tenth Circuit and Fifth Circuits have interpreted this language as precluding liability for aiders and abettors. *See Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1246 (10th Cir. 2012); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th Cir. 2000); *but see Longan v. Hasty*, 436 F. Supp. 2d 419, 427-28 (E.D.N.Y. 2006) (concluding that § 2520 permits suits based on procurement). In their analysis, the Tenth and Fifth Circuits point to the fact that a prior version of the law “imposed both criminal and civil liability for those who *procured* an interception.” *Kirch*, 702 F.3d at 1247 (citing 18 U.S.C. § 2511(1)(a) (1968)) (emphasis added). However, an amendment in 1986 removed the procurement language from the civil liability provision, limiting civil liability to the person that “engaged in that violation.” *Peavy*, 221 F.3d at 169 (quoting 18 U.S.C. § 2520(a)) (“Accordingly, ‘that violation’ refers only to illegal interception, disclosure, or use, and *not* to procuring interception by another.”) (emphasis in original).

While the Fourth Circuit has not addressed whether § 2520 authorizes suits based on procurement, *see Attkisson v. Holder*, 925 F.3d 606, 623 (4th Cir. 2019), *as amended* (June 10, 2019) (acknowledging “lack of settled precedent” on this issue), several district courts in this Circuit have followed the Tenth and Fifth Circuits’ reasoning. *See Motise v. Am. Online, Inc.*, No. CIV.A. 04-1494, 2005 WL 1667658, at *4 (E.D. Va. June 24, 2005) (dismissing plaintiff’s claim because the Wiretap Act “does not recognize a cause of action for aiding and

abetting a primary violator, and the Act does not create any secondary liability” and plaintiff only alleged that defendant enabled a third party to intercept communications, rather than alleging that defendant intercepted such communications itself); *Buckingham v. Gailor*, No. 00-CV-1568, 2001 WL 34036325, at *6 (D. Md. Mar. 27, 2001), *aff’d sub nom. Buckingham ex rel. Buckingham v. Gailor*, 20 F. App’x 243 (4th Cir. 2001) (concluding that an action based on procurement “is no longer available under 18 U.S.C. § 2520, as a result of amendments passed by Congress in 1986”). The undersigned is persuaded by the reasoning of these courts and finds that the weight of authority supports dismissing Wiretap Act claims based on procurement.

Plaintiff argues in response that Defendants are primarily liable under the Wiretap Act because they themselves “disclosed and endeavored to disclose” Plaintiff’s intercepted communications. (Docket Entry 34 at 14.) To support this argument, Plaintiff points to allegations in the complaint stating that Defendants were hired to hack Plaintiff and were part of a plan to attack him. (*Id.* (citing Compl. ¶¶ 14-15.) However, in the allegations supporting Plaintiff’s Wiretap claim brought pursuant to 18 U.S.C. § 2511(1)(c), Plaintiff clearly alleges that Defendants “directed CyberRoot to intentionally disclose large quantities of Azima’s intercepted data” and that CyberRoot created the blog sites where the data was published and uploaded the stolen data. (Compl. ¶¶ 49-52 (“[Defendants] gave the instructions to CyberRoot to intercept Azima’s data and paid CyberRoot more than \$1 million to conduct the hack and publish the stolen data.”).⁶ These allegations clearly show

⁶ To the extent that the complaint contains other general allegations that Defendants were personally involved in the interception and disclosure of Plaintiff’s data, such allegations lack the particularity required to state a plausible claim for relief and conflict with other more specific

that Defendants *procured* CyberRoot to intercept Plaintiff's stolen data and did not engage in the interception themselves. The undersigned therefore recommends dismissing Count I of Plaintiff's complaint on this basis and will not address Defendants' alternative arguments for dismissal of this claim.

b. Conspiracy in violation of the Wiretap Act (Count II)

Count II of Plaintiff's complaint raises a claim for conspiracy to disclose and use intercepted communications in violation of the Wiretap Act and 18 U.S.C. § 371. (*See* Compl. ¶¶ 54-58.) Plaintiff alleges that Defendants conspired with CyberRoot and others to intercept and disclose Plaintiff's data. (*Id.* ¶ 55.) More specifically, Plaintiff alleges that "Defendants Del Rosso and Vital paid more than \$1 million for the interception of Azima's data [and] agreed and conspired to disclose the intercepted data by instructing CyberRoot to publish the data on blog sites that were created by CyberRoot." (*Id.*)

In their brief in support of their motion to dismiss, Defendants addressed Counts I and II simultaneously, arguing as described above that the Wiretap Act precludes liability for secondary or conspiracy conduct, in addition to raising two other arguments involving extraterritoriality and Plaintiff's failure to plead "interception." (*See* Docket Entry 32 at 16-19.) The undersigned finds, however, that Plaintiff's Count II should be dismissed because 18 U.S.C. § 371 is a federal criminal statute that does not provide Plaintiff with a private cause of action. *See, e.g., Sanders v. GNC Holdings, Inc.*, No. 5:20-CV-00238-D, 2020 WL

allegations in the complaint attributing this conduct to CyberRoot. (*See, e.g.,* Compl. ¶ 92 ("Defendants knowingly broadcast or published personal information of Azima on the internet."); *but see id.* ¶¶ 19-32 (alleging that Defendants paid CyberRoot \$1 million to hack and distribute Plaintiff's data and that CyberRoot used specific usernames to create blog sites and upload the data).)

5792462, at *3 (E.D.N.C. July 8, 2020), *report and recommendation adopted*, No. 5:20-CV-238-D, 2020 WL 5770851 (E.D.N.C. Sept. 28, 2020) (“A federal prosecutor could bring charges against a defendant for conspiracy to commit an offense against or an attempt to defraud the United States, but 18 U.S.C. § 371 does not create a private cause of action.”); *Bey ex rel Graves v. Richmond Redevelopment & Hous. Auth.*, No. 3:13CV464-HEH, 2013 WL 4066945, at *5 (E.D. Va. Aug. 9, 2013) (“18 U.S.C. § 371 criminalizes the act of conspiring to commit a crime against the United States; it does not create a cause of action for individuals alleging conspiracy.”). Thus, the undersigned recommends that Count Two of Plaintiff’s complaint be dismissed for failure to state a claim.

c. Misappropriation of Trade Secrets (Count III)

Plaintiff raises a claim for misappropriation of trade secrets against Defendants pursuant to the Defend Trade Secrets Act (“DTSA”), 18 U.S.C. §§ 1831, 1832, 1836. (*See* Compl. ¶¶ 59-74.) As Defendants have properly argued (*see* Docket Entry 32 at 20 n. 9), 18 U.S.C. §§ 1831 and 1832 are federal criminal statutes that do not provide a private right of action. *See, e.g., Rogers v. LJT & Assocs. Inc.*, No. CV GLR-14-2823, 2015 WL 11027599, at *3 n. 4 (D. Md. Apr. 21, 2015); *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 271 F. Supp. 3d 835, 840-43 (E.D. Va. 2017); *Lopez v. MUFG Union Bank, N.A.*, No. SACV151354JLSKESX, 2016 WL 9686990, at *6 (C.D. Cal. Mar. 30, 2016) (“Claims under sections 1831 and 1832 of Title 18 invoke a criminal statute without a private right of action.”). Thus, any action brought by Plaintiff under these provisions fail to state a claim and should be dismissed at the outset.

Section 1836(b)(1) of the DTSA provides that “[a]n owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to

a product or service used in, or intended for use in, interstate or foreign commerce.” Thus, to prevail on a misappropriation claim, Plaintiff must allege that: “(1) [he] owns a trade secret which was subject to reasonable measures of secrecy; (2) the trade secret was misappropriated by improper means; and (3) the trade secret implicates interstate or foreign commerce.” *Philips N. Am. LLC v. Hayes*, No. CV ELH-20-1409, 2020 WL 5407796, at *7 (D. Md. Sept. 9, 2020).

Defendants argue that Count III fails to state a claim because: 1) the DTSA does not provide for conspiracy liability; 2) Plaintiff has not alleged with the required specificity that his hacked data contained trade secrets or implicated interstate or foreign commerce; and 3) Plaintiff’s claim is barred because the misappropriation he complains of occurred prior to the DTSA’s enactment May 2016. (*See* Docket Entry 32 at 19-22.)

In making their first argument, Defendants rely on *Steves & Sons, Inc. v. JELD-WEN, Inc.*, in which the Eastern District of Virginia, engaged in statutory interpretation and determined that a private right of action does not exist under 18 U.S.C. § 1832(a)(5), which prohibits conspiracy to engage in the theft of trade secrets. *See* 271 F. Supp. 3d at 840-43. Several federal district courts have agreed with *JELD-WEN’s* interpretation and have dismissed civil DTSA claims to the extent that they were based on conspiracy or secondary liability. *See Genentech, Inc. v. JHL Biotech, Inc.*, No. C 18-06582 WHA, 2019 WL 1045911, at *12 (N.D. Cal. Mar. 5, 2019); *Broidy Cap. Mgmt. LLC v. Muzin*, No. 19-CV-0150 (DLF), 2020 WL 1536350, at *13 (D.D.C. Mar. 31, 2020); *C-Ville Fabricating, Inc. v. Tarter*, No. 5:18-CV-379-KKC, 2019 WL 1368621, at *14 (E.D. Ky. Mar. 26, 2019). While definitive binding authority on this issue is lacking, the undersigned agrees that “the weight of authority tips

against the viability of conspiracy claims based on misappropriation of trade secrets under the DTSA.” *NW Monitoring LLC v. Hollander*, No. C20-5572 RSM, 2021 WL 1424690, at *5 (W.D. Wash. Apr. 15, 2021). Thus, to the extent that Plaintiff’s DTSA claim is based on the actions of co-conspirators (*see* Compl. ¶¶ 70-73), the undersigned recommends that this theory of liability not be permitted going forward. *See Broidy Cap. Mgmt. LLC*, 2020 WL 1536350, at *13.

However, here, Plaintiff has argued that Defendants are also primarily liable under the DTSA because they themselves obtained Plaintiff’s trade secrets. (*See* Docket Entry 34 at 17.) The DTSA defines misappropriation as the “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.” 18 U.S.C. § 1839(5)(A). Plaintiff’s complaint clearly alleges that Defendants knew Plaintiff’s trade secrets were acquired improperly, in addition to alleging that “at least some of that data [that CyberRoot obtained through the hacking] was provided to Del Rosso, who was located in North Carolina.” (Comp. ¶ 19.) Thus, Plaintiff has sufficiently alleged the element of misappropriation as to Defendants.

Second, the undersigned finds that Plaintiff has alleged his ownership of trade secrets and their implication in interstate or foreign commerce with sufficient particularity at this early stage in the litigation. The DTSA’s definition of trade secrets is broad. *See* 18 U.S.C. 1839(3) (defining trade secrets as “all forms and types of financial, business, scientific, technical, economic, or engineering information” that the owner has taken reasonable measure to keep secret and that derives independent economic value from its secrecy). In addition, the DTSA does not “include an express requirement that a plaintiff identify its

trade secret with reasonable particularity to state a claim. Thus, to survive a motion to dismiss under the DTSA . . . a claimant ‘need only plausibly plead’ that a defendant acquired the trade secrets at issue by improper means.” *Heska Corp. v. Qorvo US, Inc.*, No. 1:19CV1108, 2020 WL 5821078, at *4 (M.D.N.C. Sept. 30, 2020) (quoting *OROS, Inc. v. Dajani*, No. 1:19-cv-351, 2019 WL 2361047, at *5 (E.D. Va. June 4, 2019)).

Plaintiff alleges that his trade secrets included private email communications, banking records, “highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, . . . contacts for important business relationships,” “confidential internal pricing lists” and “spreadsheets connected to contracts with the United States government” relating to food transport for U.S. troops in Afghanistan. (Compl. ¶¶ 18, 52, 102, 108.) Plaintiff alleges that he “has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software” and that his trade secrets derive economic value from not being generally known. (*Id.* ¶¶ 66-67.) Furthermore, to the extent that Plaintiff has alleged that his business involves the transportation of supplies to Afghanistan, he has sufficiently established the interstate or foreign commerce element of his claim. *See Philips N. Am. LLC*, 2020 WL 5407796, at *11 (“At the motion to dismiss stage, it is sufficient that [plaintiff] alleges that its . . . business is both national and international. As a result, the court may easily infer that the purported information relates to services used and intended for use in interstate and foreign commerce.”). Thus, Plaintiff has plausibly pled his ownership of trade secrets.

Third, while Plaintiff's complaint does not state definitively when the misappropriation of his information occurred, there are allegations suggesting that it happened in or around August 2016, several months after the DTSA's May 2016 enactment. (*See* Compl. ¶¶ 20-21, 32, 35.) For these reasons, the undersigned does not recommend dismissing Plaintiff's misappropriation of trade secrets (Count III) claim at this stage with the caveat that Plaintiff not be permitted to advance theories of conspiracy or secondary liability going forward. *See Broidy Cap. Mgmt. LLC*, 2020 WL 1536350, at *13 (“[Plaintiff] must prove that each defendant *individually* misappropriated at least one trade secret.”) (emphasis added).

d. Identity Theft (Count VI)

Plaintiff brings claim for identity theft pursuant to N.C. Gen Stat. §§ 14-113.20 and 1-539.2C. (*See* Compl. ¶¶ 86-90.) Section 14-113.20 is a state criminal statute providing that

A person who knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to fraudulently represent that the person is the other person for the purposes of making financial or credit transactions in the other person's name, to obtain anything of value, benefit, or advantage, or for the purpose of avoiding legal consequences is guilty of a felony.

N.C. Gen Stat. § 14-113.20(a). Section 14-113.22(b) provides that “any person who commits an act made unlawful by Section 14-113.20 “may also be liable for damages under [Section] 1-539.2C.” Section 1-539.2C creates a private right of action for “[a]ny person whose property or person is injured by reason of an act made unlawful by Article 19C of Chapter 14 of the General Statutes”

Defendants argue that Plaintiff's Complaint fails to state a claim for identity theft because it "does not allege that Defendants used any of his 'identifying information' to 'fraudulently represent' to others that they were Azima." (Docket Entry 32 at 23.) In response, Plaintiff points to his allegation in the complaint that Defendants hacked Plaintiff's computer network to obtain his passwords and other information "with the intent to fraudulently represent that Defendants were the Plaintiff for the purposes of obtaining materials of value, benefit, and advantage." (Docket Entry 34 at 19 (quoting Compl. ¶ 87).)

While Plaintiff has properly recited the language of the statute, a cause of action must contain more than "a formulaic recitation of the elements" to survive a motion to dismiss. *Atlantic v. Twombly*, 550 U.S. 544, 555 (2007). Plaintiff has alleged that Defendants orchestrated the sending of phishing and spear phishing emails to obtain access to Plaintiff's accounts, but the undersigned cannot identify specific factual allegations in the complaint demonstrating that Defendants made representations to any other individual or entity that they were Plaintiff. Therefore, Plaintiff has not plausibly stated a claim for relief on the basis of identity theft and this claim should be dismissed. *See Best v. Cequel*, No. 4:14-CV-61-FL, 2014 WL 6453960, at *4 (E.D.N.C. Nov. 17, 2014), *aff'd*, 598 F. App'x 178 (4th Cir. 2015) (dismissing plaintiff's identity theft claim where complaint failed to allege that defendants "used plaintiff's identifying information with the intent to fraudulently represent themselves as plaintiff, as required by N.C. Gen. Stat. § 14-113.20").

e. Publication of Personal Information (Count VII)

Plaintiff brings this claim pursuant to N.C. Gen. Stat. § 75-66 (*see* Compl. ¶¶ 91-100), which provides that

It shall be a violation of this section for any person to knowingly broadcast or publish to the public on radio, television, cable television, in a writing of any kind, or on the Internet, the personal information of another with actual knowledge that the person whose personal information is disclosed has previously objected to any such disclosure.

Defendants argue that Plaintiff's complaint fails to state a claim for relief under this statute because "he does not allege that he previously objected to the disclosure of any such information or that Defendants had 'actual knowledge' of such an objection, both of which are required to state a claim under the statute." (Docket Entry 32 at 23.) Plaintiff responds that Defendants published Plaintiff's personal information on blog sites in 2018 and 2019 after Plaintiff "responded to the complaint in England by claiming his data was illegally hacked." (Docket Entry 34 at 19 (citing Compl. ¶ 93; Docket Entry 31-2 at 13 (judgment in English proceeding)). By referring to the judgment in the English case attached as an exhibit to Defendants' motion to dismiss, Plaintiff concedes that his complaint does not contain facts to support the objection element of his publication claim. A court may consider matters of public record when considering a motion to dismiss. *U.S. ex rel. Oberg v. Pennsylvania Higher Educ. Assistance Agency*, 745 F.3d 131, 136 (4th Cir. 2014) ("[I]n reviewing a Rule 12(b)(6) dismissal . . . we may properly take judicial notice of matters of public record, including statutes.") (internal quotations omitted). However, the first page of the judgment Plaintiff refers to makes it clear that neither Del Rosso nor Vital were named as defendants in that lawsuit. (See Docket Entry 31-2 at 1 (listing RAKIA as the sole defendant).) Plaintiff has alleged that Defendant Del Rosso provided a witness statement and witness testimony in the English lawsuit (see Compl. ¶ 8), but there is no indication that he did those things prior to the publication of his stolen data in 2018 and 2019. (See Docket Entry 31-2 (indicating

that hearings for the case not held until January and February 2020).) Thus, to the extent that Plaintiff's response to RAKIA in the English lawsuit could constitute an objection to the disclosure of his information, the undersigned cannot plausibly infer that Defendants had actual knowledge of such an objection before they committed any of the alleged disclosures of Plaintiff's personal information. Therefore, the undersigned recommends dismissing this claim. *See In re Winter*, 2015 WL 5063953, at *3 (Bankr. E.D.N.C. Aug. 26, 2015) (dismissing publication of personal information claim because "the Plaintiffs have not provided evidence of any prior objection to the disclosure of their personal information").

f. Violation of Trade Secrets Protection Act (Count VIII)

Plaintiff brings this claim pursuant to the North Carolina Trade Secrets Protection Act ("TSPA"), N.C. Gen. Stat. § 66-153 *et seq.* (*See* Compl. ¶¶ 101-18.) Defendants argue that Plaintiff's claim fails because he has not identified a trade secret with sufficient particularity. (Docket Entry 32 at 24.) Defendants are correct that to state a claim for violation of the TSPA, "[t]he alleged trade secret information must be identified 'with sufficient particularity so as to enable a defendant to delineate that which he is accused of misappropriating and a court to determine whether misappropriation has or is threatened to occur.'" *Asheboro Paper & Packaging, Inc. v. Dickinson*, 599 F. Supp. 2d 664, 676 (M.D.N.C. 2009) (quoting *Analog Devices, Inc. v. Michalski*, 579 S.E.2d 449, 453 (N.C. Ct. App. 2003)). However, "[c]ustomer pricing lists, cost information, confidential customer lists, and pricing and bidding formulas can constitute trade secrets." *Sunbelt Rentals, Inc. v. Head & Engquist Equip., L.L.C.*, 620 S.E.2d 222, 226 (N.C. Ct. App. 2005).

As discussed above under the analysis for Plaintiff's federal misappropriation of trade secrets claim, Plaintiff has alleged that his trade secrets included "confidential internal price lists and confidential spreadsheets connected to contracts with the United States government to supply troops in Afghanistan." (Compl. ¶ 108.) Therefore, the undersigned finds that Plaintiff has alleged violation of the TSPA with sufficient particularity at this early stage in the litigation and does not recommend dismissing Count VIII of Plaintiff's complaint.

g. Unfair and Deceptive Trade Practices (Count IX)

Plaintiff brings his ninth claim pursuant to North Carolina's Unfair and Deceptive Trade Practices Act ("UDTPA"), N.C. Gen. Stat. § 75-1.1 *et seq.* (See Compl. ¶¶ 119-29.) The UDTPA prohibits "unfair or deceptive acts or practices in or affecting commerce." N.C. Gen. Stat. § 75-1.1(a). Defendants argue that Plaintiff fails to state a claim under the UDTPA because "he has not sufficiently alleged an unfair or deceptive act or practice by Defendants or that any such act had the capacity or tendency to deceive the average consumer," and that Plaintiff fails to allege that Defendants' deceptive practices arose from commercial activities "in or affecting commerce." (Docket Entry 32 at 25 (internal quotations omitted).)

"The North Carolina Supreme Court has held that § 75-1 is intended to 'regulate two types of interactions in the business setting: (1) interactions between businesses, and (2) interactions between businesses and consumers.'" *McClean v. Duke Univ.*, 376 F. Supp. 3d 585, 608 (M.D.N.C. 2019) (quoting *White v. Thompson*, 691 S.E.2d 676, 679-80 (N.C. 2010)). While the statute "affords broad relief to individual consumers," North Carolina courts "have viewed the rights of businesses to sue other businesses for violations of the UD[T]PA

with a much more skeptical eye.” *Exclaim Mktg., LLC v. DirecTV, LLC*, 134 F. Supp. 3d 1011, 1020 (E.D.N.C. 2015), *aff’d*, 674 F. App’x 250 (4th Cir. 2016); *see also Dalton v. Camp*, 548 S.E.2d 704, 710 (N.C. 2001) (“The [UDTPA] was intended to benefit consumers . . . but its protections extend to businesses in appropriate situations.”). Indeed, the statute “gives a business a cause of action against another business only where: 1) the plaintiff-business is in the marketplace acting as a consumer or is otherwise engaged in commercial dealing with defendant, 2) the businesses are competitors, or 3) the conduct giving rise to the cause of action has a negative effect on the consuming public.” *Id.* (internal quotations omitted).

Here, Plaintiff describes himself as “a successful businessman who has owned and operated multiple aviation related companies,” while Defendant Del Rosso is the owner of Defendant Vital, which provides investigative services. (Compl. ¶¶ 10-11.) The complaint does not contain any allegation that Plaintiff was engaged in commercial dealing with Defendants or that Plaintiff’s companies and Vital are competitors. Nor has Plaintiff alleged that the deceptive acts by Defendants have negatively affected the consuming public. Indeed, Plaintiff only alleges injury to himself as a result of Defendants’ acts. (*Id.* ¶¶ 126-27.) For these reasons, the undersigned concludes that Plaintiff has failed to allege that Defendants engaged in the type of deception that the UDTPA is intended to prevent. *See Prince v. Wright*, 541 S.E.2d 191, 197 (N.C. Ct. App. 2000) (“[T]he fundamental purpose of G.S. § 75–1.1 is to protect the consuming public.”). Therefore, it is recommended that Count IX of Plaintiff’s complaint be dismissed.

h. Civil Conspiracy (Count X)

Plaintiff's tenth cause of action is one for civil conspiracy pursuant to North Carolina common law. (*See* Compl. ¶¶ 130-35.) Plaintiff alleges that Defendants and their co-conspirators “wrongfully entered into an agreement to commit unlawful acts resulting in injury to Azima” (*Id.* ¶ 131.) Defendants argue that this claim should be dismissed because “there is no standalone claim for civil conspiracy under North Carolina law,” and that Plaintiff has made only conclusory assertions that there was a conspiracy between Defendants and others. (Docket Entry 32 at 26.)

While it is true that under North Carolina law “[t]here is no independent cause of action for civil conspiracy,” a plaintiff may state a claim for civil conspiracy where there is an underlying claim for unlawful conduct and the plaintiff has alleged “the agreement of two or more parties to carry out the conduct and injury resulting from that agreement.” *Toomer v. Garrett*, 574 S.E.2d 76, 92 (N.C. Ct. App. 2002); *see also Swain v. Elfland*, 387, 550 S.E.2d 530, 534 (N.C. Ct. App. 2001) (“A claim for conspiracy . . . cannot succeed without a successful underlying claim”) (alterations in original).

Here, the undersigned has found that Plaintiff has successfully plead claims for misappropriation of trade secrets, violation of the Trade Secrets Protection Act, and invasion of privacy. (*See* Sections I.A.2(c) and (f) *supra* and Section 1.A.2.(i) *infra*.) Furthermore, Plaintiff has adequately alleged an agreement between Defendants, Dechert LLP, and CyberRoot and an injury to himself resulting from that agreement. Plaintiff alleges that Dechert LLP hired and paid Defendants “more than \$1 million” to hack him. (Compl. ¶¶ 1-2, 7, 13, 27-28.) Plaintiff also alleges that “Defendants paid CyberRoot more than \$1

million for the hacking of Azima and the dissemination of his stolen data” and directed CyberRoot to send phishing emails to Plaintiff. (*Id.* ¶ 5; *see also id.* ¶¶ 20, 29-32.) However, the undersigned agrees with Defendants that Plaintiff has not adequately alleged an agreement between Defendants and BellTroX. (*See id.* ¶¶ 16-17 (indicating that “CyberRoot was assisted by BellTroX” and that the companies “share common employees” but making no allegations that Defendants paid or directly communicated with BellTroX about the hacking).) For these reasons, the undersigned finds that Plaintiff has stated a plausible claim for civil conspiracy based on an agreement between Defendants, Dechert LLP, and CyberRoot, and therefore does not recommend dismissing Count X of Plaintiff’s complaint at this time.

i. Invasion of Privacy by Intrusion into Seclusion (Count XI)

Plaintiff’s final claim is for invasion of privacy by intrusion into seclusion, which he brings pursuant to North Carolina common law. (*See id.* ¶¶ 136-39.) “North Carolina recognizes the tort of intrusion of seclusion when ‘[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.’” *Musenge v. SmartWay of the Carolinas, LLC*, No. 3:15-CV-153-RJC-DCK, 2018 WL 4440718, at *5 (W.D.N.C. Sept. 17, 2018) (quoting *Miller v. Brooks*, 472 S.E.2d 350, 354 (N.C. Ct. App. 1996)). Defendants argue that dismissal of this claim is warranted because Plaintiff “has not alleged an intrusion into his personal affairs that is highly offensive to a reasonable person.” (Docket Entry 32 at 25 (internal quotations omitted).)

“Generally, there must be a physical or sensory intrusion or an unauthorized prying into confidential personal records to support a claim for invasion of privacy by intrusion.” *Broughton v. McClatchy Newspapers, Inc.*, 161 N.C. App. 20, 29, 588 S.E.2d 20, 27 (2003); *see also Berg v. Murratti*, No. 3:17CV491, 2017 WL 5340383, at *2 (W.D.N.C. Nov. 13, 2017) (quoting *Toomer*, 574 S.E.2d at 90) (“Examples of recognized intrusions upon seclusion include ‘physically invading a person’s home or other private place, eavesdropping by wiretapping or microphones, peering through windows, persistent telephoning, unauthorized prying into a bank account, and opening personal mail of another.’” *Berg v. Murratti*, No. 3:17CV491, 2017 WL 5340383, at *2 (W.D.N.C. Nov. 13, 2017) (quoting *Toomer*, 574 S.E.2d at 90)). Plaintiff has alleged that Defendants accessed his “confidential business information, and personal information and communications” such as “confidential legal communications and advice and confidential internal pricing lists” by directing the hacking of his email accounts and computers. (*See, e.g.*, Compl. ¶ 16-18, 90.) At the motion to dismiss stage, the undersigned finds that these allegations are sufficient to state a plausible claim for intrusion into seclusion. Therefore, the undersigned recommends denying Defendants’ motion to dismiss as to Count XI of Plaintiff’s complaint.

In summary, the undersigned recommends denying Defendants’ motion to dismiss as to Plaintiff’s claims for misappropriation of trade secrets (Count III), violation of the Trade Secrets Protection Act (Count VIII), civil conspiracy (Count X), and intrusion into seclusion (Count XI). As to Plaintiff’s other seven claims, the undersigned recommends granting Defendants’ motion for the reasons stated herein.

B. Plaintiff's motion for leave to supplement his response to Defendants' motion to dismiss

In this motion, Plaintiff asks the Court to consider newly discovered bank records in its analysis of Defendant's motion to dismiss. (Docket Entry 45.) Defendants filed a response in opposition to Plaintiff's motion. (Docket Entry 47.) Apparently records from Kotak Mahindra Bank were submitted to this Court in conjunction with an *ex parte* application for an order under 28 U.S.C. § 1782 to serve subpoenas on Defendants to obtain discovery materials for use in legal proceedings in the United Kingdom. (*Id.* at 2 (referencing *In Re Application of Al Sadeq and Stokoe Partnership Solicitors*, No. 1:21-MC-00006 (M.D.N.C. Feb. 5, 2021)).) According to Plaintiff's motion, these records show 51 payments received by CyberRoot from Defendant Vital between 2016 and 2017 totaling more than \$1 million. (*Id.* at 2-3.) Plaintiff contends that these records controvert Defendants' denial of Plaintiff's allegations that they were involved in ongoing conduct related to the hacking continuing into 2019. (*Id.* at 4.) Plaintiff asserts that by making this denial, "Defendants have opened the door to the Court's considering the newly discovered bank records in connection with Defendants' pending motion [to dismiss]." (*Id.*)

First, at the motion to dismiss stage, the "court accepts all well-pled facts as true and construes these facts in the light most favorable to the plaintiff." *Nemet Chevrolet, Ltd.*, 591 F.3d at 255. As Defendants properly point out (*see* Docket Entry 47 at 8), Plaintiff's complaint already contains repeated allegations that Defendants paid CyberRoot \$1 million. (Compl. ¶¶ 5, 29, 52, 55, 57, 73, 79, 85, 115, 133.) Plaintiff has also alleged that the payments "made by Vital were sent to Cyber Root's bank, Kotak Mahindra Bank . . . around the time that Azima's stolen data was published online in August and September 2016." (*Id.*

¶¶ 31-32.) Therefore, because the bank records merely duplicate allegations already contained in Plaintiff's complaint, the Court sees no reason to consider them at this stage. *See Cabrera Mejia v. Wal-Mart*, No. 1:14CV237, 2014 WL 5531432, at *2 (M.D.N.C. Nov. 3, 2014), *aff'd sub nom. Mejia v. Wal-Mart*, 599 F. App'x 520 (4th Cir. 2015) ("Because these filings provide no new factual allegations but simply repeat allegations from the complaint and its attachments, this court need not determine whether it should consider those later-filed documents.")

Second, "[e]ven though matters outside the pleadings are generally not considered on a Rule 12(b)(6) motion, . . . the court can consider documents attached to the complaint, documents incorporated by reference in the complaint, or matters of judicial notice without converting a motion to dismiss into one for summary judgment." *Shore v. Charlotte-Mecklenburg Hosp. Auth.*, 412 F. Supp. 3d 568, 573 (M.D.N.C. 2019), *appeal dismissed*, No. 19-2086, 2019 WL 8359567 (4th Cir. Dec. 16, 2019) (internal quotations and citations omitted). "The court may take judicial notice of public documents and government documents because their sources cannot reasonably be questioned." *Id.* (internal quotations omitted); *see also* Fed. R. Evid. 201(b) ("The court may judicially notice a fact that is not subject to reasonable dispute because it: (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned."). However, the bank records Plaintiff asks the Court to consider were not exhibits attached to the complaint nor were they incorporated by reference therein. Furthermore, the bank records are not a matter of public record nor is their accuracy beyond question. The Court cannot take judicial notice of the bank records

and therefore cannot properly consider them at this time. For these reasons, the Court will deny Plaintiff's motion.

C. Plaintiff's motions to schedule an initial pretrial conference or commence discovery

Shortly after Defendants filed their motion to dismiss, Plaintiff filed a motion asking the Court "to schedule an initial pretrial conference and to initiate Rule 26(f) and Local Rule 16.1(f) conferences and reporting process," or alternatively, "issue an order commencing discovery pending a pretrial conference to be set on a later date." (Docket Entry 36 at 1.) Plaintiff states that because several months have passed since he filed his complaint, further delays in commencing discovery are not warranted by good cause or the federal and local rules. (Docket Entry 37 at 3.) Defendants responded in opposition, noting that there is "no obligation for the parties to hold a Rule 26(f) conference where the initial pretrial conference had not yet been scheduled." (Docket Entry 43 at 8-9 (citing *Williams v. Pegasus Residential, LLC*, 2019 WL 8586707, at *1 (M.D.N.C. May 3, 2019).)

On July 1, 2021, Plaintiff filed a renewed motion to schedule an initial pretrial conference or otherwise commence discovery. (Docket Entry 52.) In addition to renewing the arguments made in his prior motion, Plaintiff also states that he urgently seeks leave to serve third-party subpoenas on Bank of America to obtain records showing payments between Dechert LLP and Defendants dating back to August 2014. (*Id.* at 4.) Plaintiff states that these records that will not be retained after August 31, 2021, per the bank's seven-year retention policy. (*Id.* at 4.) Defendants oppose this motion as procedurally improper. (Docket Entry 53 at 4 ("The relevant Federal and local rules of civil procedure provide no avenue for a party to make a motion to 'renew' an already-filed and referred motion.").)

Defendants also argue that Plaintiff has not shown why Bank of American records dating back to 2014 are relevant to his claims, and that in any case, it is “in the Court’s discretion to address the pending dispositive motion before scheduling an initial pretrial conference or authorizing discovery to commence.” (*Id.* at 4-5.)

Federal Rule of Civil Procedure 26 requires parties to “confer as soon as practicable-- and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b)” unless “the court orders otherwise.” Fed. R. Civ. P. 26(f). Local Rule 16.1(b) provides that “the parties must hold their [Rule] 26(f) meeting at least 14 days before the scheduled initial pretrial conference and submit to the Court their report within 10 days thereafter.” M.D.N.C. LR 16.1(b). In addition, the Court has discretionary authority to manage its own docket. *See Landress v. Tier One Solar LLC*, 243 F. Supp. 3d 633, 646 (M.D.N.C. 2017) (internal quotation and citation omitted) (“Proper use of this authority requires the court to exercise its judgment to balance the various factors relevant to the expeditious and comprehensive disposition of the causes of action on the court's docket.”); *Marryshow v. Flynn*, 986 F.2d 689, 693 (4th Cir. 1993) (“[B]road discretion is given to the trial court to manage its docket.”).

Here, the Court has not scheduled an initial pretrial conference, nor have Defendants filed an answer in this matter. The undersigned magistrate judge has recommended herein the dismissal of several of Plaintiff's claims. However, this recommendation awaits a final ruling by the district court judge, which will determine the scope of the case going forward. Given the general local practices in this district and considering the Court’s discretionary authority to manage its cases on its docket, the Court finds that it is not “practicable” for the

parties to confer regarding discovery at this time. The Court declines to schedule an initial pretrial conference or otherwise order the commencement of general discovery before there has been a final ruling on Defendants' motion to dismiss.

However, according to Plaintiff's representations, Plaintiff's ability to subpoena records showing payments between Defendants and Dechert LLP in the possession of third-party Bank of America may be limited after August 31, 2021. (*See generally* Docket Entry 52.) Such documents may have some bearing on Plaintiff's civil conspiracy claim (for which the undersigned has not recommended dismissal) insofar as Plaintiff has alleged a conspiracy between Defendants and Dechert LLP. (*See* Compl. ¶¶ 13, 133.) Accordingly, the Court will allow a brief period of very limited discovery so that Plaintiff may serve these subpoenas upon third-party Bank of America. Plaintiff's must serve the subpoenas upon Bank of America on or before August 31, 2021, pursuant to the Federal Rule of Civil Procedure and this Court's local rules. No further discovery is permitted at this time. In all other respects, Plaintiff's requests to schedule an initial pretrial conference and commence discovery are denied.

III. CONCLUSION

IT IS HEREBY RECOMMENDED that Defendants' motion to dismiss (Docket Entry 31) be **DENIED IN PART** as to Counts III, VIII, X, and XI of Plaintiff's complaint, but **GRANTED IN PART** as to Plaintiff's other seven claims.

IT IS HEREBY ORDERED that Plaintiff's motion for leave to file supplemental materials in support of his response to Defendants' motion to dismiss (Docket Entry 45) is **DENIED**.

IT IS FURTHER ORDERED Plaintiff's motion to schedule an initial pretrial conference and initiate Rule 26(f) and Local Rule 16.1(f) conferences, or in the alternative, for an order commencing discovery pending a pretrial conference to be set on a later date (Docket Entry 36) and his renewed motion for the same purpose (Docket Entry 52) are **GRANTED IN PART** to the extent that on or before August 31, 2021, Plaintiff may serve subpoenas on third-party Bank of America requesting records of payments between Defendants and Dechert LLP. In all other respects, Plaintiff's two motions (Docket Entries 36 and 52) are **DENIED**.

A handwritten signature in black ink, appearing to read "Joe L. Webster", is written over a horizontal line.

Joe L. Webster
United States Magistrate Judge

August 9, 2021
Durham, North Carolina